AMENDMENTS TO THE CLAIMS

The following is a complete, marked-up listing of revised claims with a status identifier in parenthesis, underlined text indicating insertions, and strike through and/or double-bracketed text indicating deletions.

LISTING OF CLAIMS

1. (Currently Amended) A method of controlling pairing between a removable security module and a host apparatus connected to the removable security module, the pairing method securing data exchanged between the removable security module and the host apparatus by using a unique pairing key, the method comprising~~A pairing control method between a first device and a second device, the pairing control method aiming to secure the data exchange with the aid of a unique pairing key, the pairing control method comprising~~:

- verifying the pairing between the removable security module and the host apparatus~~two devices~~ and using the unique pairing key when the pairing between the removable security module and the host apparatus~~two devices~~ has been already carried out, wherein, when the pairing~~paring~~ between the removable security module and the host apparatus~~two devices~~ has not been carried out, the method includes,

- searching for a free location among ~~the~~ locations reserved for the unique pairing key in the removable security module~~first device~~ and wherein, when a free location is absent, the method further includes performing at least one of

reading an activity counter associated with each location of the removable security module~~first device~~, said activity counter being incremented each time a location is used for pairing, and finding a lowest value activity counter to determine the location to be used for a pairing procedure, and

reading a chronology counter associated with each location of the removable security module~~first device~~, said chronology counter being incremented each time a location is used for pairing, and finding a lowest value chronology counter to determine the location to be used for a pairing procedure,

- initiating the pairing procedure by transmitting a cryptogram contained in the host apparatus~~second device~~, the cryptogram including an identifier identifying the host apparatus~~second device~~ and the unique pairing key, and the cryptogram being encrypted by a secret key common to a plurality of removable security modules, the plurality of removable security modules including the removable security module~~all the first devices~~,

- decrypting the cryptogram with the removable security module~~first device~~ and extracting the identifier of the host apparatus~~second device~~ and the unique pairing key from the cryptogram, and

- storing the unique pairing key in the removable security module~~first device~~, the unique pairing key used to pair with the host apparatus~~second device~~.

2. (Currently Amended) The method according to claim 1, wherein the unique pairing key is based on the identifier of the host apparatus~~second device and~~ on the data of the removable security module~~first device~~.

3. (Currently Amended) The method according to claim 1, wherein the cryptogram is stored in the removable security module~~first device~~ and encrypted with a secret key common to a plurality of host apparatuses~~second devices~~.

4. (Cancelled)

5. (Currently Amended) The method according to claim 1, wherein pairing is conditioned by the introduction of a secret code transmitted to the removable security module~~first device~~ and verified by said removable security module~~first device~~.

6. (Currently Amended) The method according to claim 5, wherein the secret code belongs to and is unique to each removable security module~~first device~~.

7. (Previously Presented) The method according to claim 5, wherein the required secret code is different in each pairing.

8. (Currently Amended) The method according to claim 5 further comprising:

- transmitting a unique identifier of the removable security module~~first device~~ and the identifier of the host apparatus~~second device~~ to a management centre~~centre~~,

- verifying the conformity of the pairing and calculating, by means of the management centre~~centre~~, a corresponding secret code on the basis of the two identifiers,

- transmitting the secret code to a user,

- initiating the pairing and requesting the introduction of the secret code, by means of the removable security module~~first device~~,

- calculating by means of the removable security module~~first device~~ the necessary secret code on the basis of the identifiers of the removable security module~~first~~ and the host apparatus~~second devices~~,

- comparing the calculated code with a code introduced by the user,

- accepting the pairing if the two codes are identical.

9. (Currently Amended) The method according to claim 8 further comprising, determining the new secret code on the basis of the ~~two~~ identifiers of the removable security module and the host apparatus and of an index that represents the number of pairings previously carried out, whereas the removable security module~~first device~~ stores this index in its memory.

10. (New) A method of controlling pairing between a removable security module and a host apparatus connected to the removable security module, the pairing method securing data exchanged between the removable security module and the host apparatus by using a unique pairing key, the method comprising:

- verifying the pairing between the removable security module and the host apparatus and using the unique pairing key when the pairing between the removable security module and the host apparatus has been already carried out, and when the pairing between the removable security module and the host apparatus has not been carried out:

- searching for a free location among locations reserved for the unique pairing key in the removable security module and wherein, when a free location is absent, the method further includes performing at least one of

reading an activity counter associated with each location of the removable security module, said activity counter being incremented each time a location is used for pairing, and finding a lowest value activity counter to determine the location to be used for a pairing procedure, and

reading a chronology counter associated with each location of the removable security module, said chronology counter being incremented each time a location is used for pairing, and finding a lowest value chronology counter to determine the location to be used for a pairing procedure,

- initiating the pairing procedure by transmitting a cryptogram contained in the host apparatus, the cryptogram including an identifier identifying the host apparatus and the unique pairing key, and the cryptogram being encrypted by a secret key common to a plurality of removable security modules, the plurality of removable security modules including the removable security module,

- decrypting the cryptogram with the removable security module and extracting the identifier of the host apparatus and the unique pairing key from the cryptogram, and

- storing the unique pairing key in the removable security module, the unique pairing key used to pair with the host apparatus.

*** END CLAIM LISTING **